REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action dated March 7, 2006. Claims 28-31 are pending. Claims 28-31 are rejected. Claim 28 has been amended. Accordingly, claims 28-31 remain pending in the present application.

This response is submitted in accordance with Rule 116 in an earnest effort to put the application in better condition for allowance. It is believed that Applicant's response has not amended the claims in a way that would raise new issues for consideration or that would require further searching of the prior art on the part of the Examiner. Arguments are also presented below that Applicant believes should render the claims allowable. In the event, however, that the Examiner is not persuaded by the arguments, it is respectfully requested that the Examiner enter the Amendment to clarify issues upon appeal.

§112 Rejection

In the Final Office Action, the Examiner rejected claim 28 because the phrase "after manufacture" renders the claim indefinite because it is not clear what is being manufactured. In response, Claim 28 has been amended to recite that master secret key K and a secret key K_i are received from a distribution center over a network after manufacture “of the PGD.”

In the Response to Arguments, the Examiner also stated that the phrase "after manufacture” in claim 28 constitutes new matter.

However, support for the amendment may be found throughout the specification, for example, on pages 1-3, 6-8, and 13. The claims of the present invention are

directed to a system that is an improvement over the prior art system described on pages 1-3 and shown in FIG. 1. Page 3 lines 6-16 describes an approach where keys shared by multiple postage generating devices are made valid for only a limited amount of time to minimize the harm created by the theft of any of the keys and to limit the time for key attack. It is specifically stated on lines 12-15 that "generating time-limited keys, however, requires that *new keys be generated periodically and distributed to the postage generating devices 14*. Because the step of distributing the keys typically occurs over the Internet or a private indications link, security for the keys becomes paramount." Thus, in this approach, the keys are generated and distributed periodically after the PGD's are installed and being used by end-users to evidence postage, which occurs "after manufacture of the PDGs".

As another example, page 13 lines 2-9 state:

> In this system, the key distribution could service the movie theater chain and issue separate keys for different venues. The operator of each local movie theater *could download new keys from the key distribution center 24 periodically (e.g., everyday). In turn, moviegoers having access to a PGD 14 would then download the master secret key and the secret key for their device group from the local movie theater via the Internet.* After receiving the keys, the PGD 14 would print and evidence movie tickets, and each movie theater would perform the verification function for verifying the tickets.

This passage clearly describes that users of PGDs can download the master secret key and the secret key for their device group periodically for printing and evidencing, which means the PGD must be installed and operating prior to receiving the keys, which is "after manufacture of the PDGs", as recited in claim 28. The text on page 7, lines 3-5, discussed in the previous Amendment in which "…the key distribution center 24 distributes the cryptographic keys to the PGDs 14 and to the distribution centers 20 via a telecommunications network" is consistent with this embodiment.

Accordingly, it is respectfully submitted that no new matter has been entered.

In the Response to Arguments, the Examiner also stated that features argued in the previous Amendment "i.e., the meters in each group destination also receive the secret corresponding to that group destination, as required by step (a), are not recited in the rejected claim(s)." Applicant traverses this statement.

Claim 28 recites that the PGD's are "**divided into n groups** identified by a group designation G_i, **i = 1,...n**. The "i" in "secret key K_i" recited in step (a) derives antecedent basis from the "group designation G_i, **i = 1,...n**". This means that there is a respective secret key for each group of PGDs, and each PGD in a group receives that respective secret key.

It is believed the Examiner failed to respond to the remaining arguments set forth in the previous Amendment. Those arguments are set forth below in their entirety. Absent any teaching or suggestion to the contrary, Applicant believes the claims of this application distinguish over the references and are in condition for allowance.

§103 Rejection

In the Office Action, the Examiner rejected claims 28-31 under 35 U.S.C. §103 (a) as being unpatentable over U.S. Patent Application No. 5,812,666 to Baker et al. in view of U.S. patent 6,058,193 to Cordery et al.

A. References Fail to Teach or Suggest All the Claim Limitations

It is respectfully submitted that the neither Baker or Cordery, singularly or in combination, teach or suggest the combination of elements recited in claim 28.

Referring to step (a), Baker fails to teach or suggest "receiving a master secret

key K and a secret key K_i from a distribution center over a network after manufacture, and storing the master secret key K and the secret key K_i in the PGD," as recited in amended claim 28.

The Examiner cites column 6, lines 50-56 and column 9, lines 33-36 of Baker for disclosing the step. These passages, however, respectively state:

> A digital meter 36 receives the vendor master key and postal master key while physically located in the vendor manufacturing facility 14 **before distribution**, and
>
> The meter is securely configured so that **once keys are installed during manufacture**, they can never be removed or determined outside the manufacturing environment without leaving physical evidence of tampering.

Accordingly, Baker fails to teach or suggest PGDs "receiving a master secret key K and a secret key K_i …over a network after manufacture," as recited in amended claim 28.

Referring to step (b) of claim 28, which recites "in response to receiving a request to generate an indicium for a mail piece destined for a particular postal destination *Dest*, generating the indicium," Baker does discuss in column 18 using a domain Master Key to generate a temporal token key to generate a token (defined as a truncated result of encrypting indicia (col. 2, lines 6-7)) from mail piece data, but it is not believed that the token is signed as required in steps (c)-(f) of claim 28, discussed below.

Referring to step (c) of claim 28, Baker fails to teach or suggest "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination." The Examiner cites column 5, lines 38-42 and column 17, lines 28-44 of Baker for teaching this step. However, these passages respectively state:

> The digital meter calculates two proof of payment tokens, one

> using the vendor master key and the other using the postal master key. Failure in the verification of either digital token is sufficient proof of fraud. Referring now to FIG. 3, vendor data center 12 provides physical and information access control for Key Management System components.
>
> ***
>
> Key registration consists of associating the country of registration, and the indicia number with the product code number and the key. The key is then stored in the country sub-domain of the install domain using a secret key that is specific to the country sub-domain. The essential feature is that the brass process that is specific to that country sub-domain relies on the install domain to install keys securely and with integrity. Keys never transfer from one install domain to another.
>
> Referring now to FIGS. 26 and 31, when the digital meter is prepared for a specific Security Domain, the Indicia Serial Number and/or Product Code Number is entered into the digital meter in message MR1. The PSR computer 34 requests registration tokens from digital meter 36 at 360. The digital meter generates two digital tokens and returns them the PSR computer at 362. The PSR computer combines the tokens with other meter information and forwards the…

These passages cited by the Examiner have nothing at all to do with "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination" and seem to be mistaken cites by the Examiner.

The Examiner further cites column 1, lines 38-50 and column 17, lines 64 through column 18, line 35 of Baker for teaching this step. However, these passages respectively state:

> In order to validate a mailpiece, that is to ensure that accounting for the postage amount printed on a mailpiece has been properly done, it is known that one may include as part of the franking an encrypted number such that, for instance, the value of the franking may be determined from the encryption to learn whether the value as printed on the mailpiece is correct. See, for example, U.S. Pat. Nos. 4,757,537 and 4,775,246 to Edelmann et al., as well as U.S. Pat. No. 4,649,266 to Eckert. It is also known to authenticate a mailpiece by including the address as a further part of the encryption as described in U.S. Pat. No. 4,725,718 to Sansone et al. and U.S. Pat. No. 4,743,747 to Fougere et al.
>
> ***
>
> Every domain has at least one sub-domain that is responsible for registering keys to indicia numbers and performing indicia verification

within that sub-domain. The Earth domain in particular has several country sub-domains. It is possible for one country to have meters in a sub-domain of the Earth domain and meters in the unique sub-domain of its own postal domain. In the example shown in FIG. 32, Country 3 has both a unique postal domain and a postal sub-domain of the earth domain. However, Country A has only meters that have keys which are installed within that country's unique postal domain.

Referring now to FIG. 27, if a digital meter is taken out of service, the information is recorded and sent to the KMS Computer 24. Key Management Computer 24 retrieves a domain master key record from the domain archive, takes a local time stamp an forwards information to Brass box 21 at 380. The Domain Master Key record is updated and forwarded to the Key Management Computer 24 at 382. The key management computer forwards the domain master key record to the domain archive and if successful returns a response to the Brass Box 21 at 384. Brass Box 21 checks response and returns a success or failure verification to Key Management Computer 24 at 386.

Generation of Tokens

Each meter uses the Domain Master Key to generate a temporal key, also referred to herein as a token key, for each domain, which is used to generate a token from mailpiece data. The Key Management System may distribute postal temporal keys to authorized postal verification sites having a Distributor Token Verification Box 44 (FIG. 1), also referred to herein as Tin Box. Postal temporal keys are used by Tin Box 44 for local verification of indicia. Under this arrangement, the Key Management System provides a higher level of security because the Post can obtain local verification of indicia without distributing the Master Key database at multiple sites.

Again these passages cited by the Examiner have nothing at all to do with "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination."

Baker also fails to teach or suggest the limitations of (d)-(f).

None of Baker's disclosed keys teach or suggest the keys and functionality of the keys described above and as recited in claim 28. For example, it is noted Baker discloses that a domain maser key is installed in each meter, and that each meter uses the domain master key to generate a temporal key, referred to as a token key, for each domain, which is used to generate a token from mail piece data. However, it is not

believed either Baker's master key or the temporal key is analogous to the verification key.

Baker's master key is not analogous because it is installed during manufacturing, not received by the PGD "over a network after manufacturing of the PDG." Because the domain master key is already present in the meter, it is also not computed as a function of "a secret key" and the postal destination, as required by step (c). The domain master key is also not used "to create a digital signature for the indicia", as recited in step (e). Instead, Baker's temporal key is used to generate the token from mail piece data. In addition, although Baker may teach that earth domain digital meters are assigned a country specific security domain and receive copies of earth domain master keys that are encrypted with a country specific secret key, Baker fails to teach or suggest that meters in each group designation, "G_i, i = 1,...n", also receive "a secret K_i," corresponding to that Group designation, as required by step (a).

It is believed Baker's temporal key is not analogous to the claimed verification key because although the temporal key is computed from one key (the domain master key), it is not computed as a function of a second key, the "secret key", and the postal destination, as required by step (c).

Moreover, it is believed that Baker's country specific secret keys cannot be considered analogous to the recited secret K_i because Baker's country specific secret keys are not believed to be installed in the meters. In addition, Baker's country specific secret keys are not used by the meters to "comput[e] a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination (*Dest*), as recited in step (c).

The Examiner relies on Cordery et al to cure the deficiencies of Baker. Cordery may teach the storing of a postal master key and a vendor master key in a meter and

using the postal and vendor master keys to generate in the meter respective postal and vendor token keys that are then used to generate respective unique postal and vendor tokens that are date dependent. However, in Cordery there is no dividing the meters into groups. Therefore, there can be no distributing a master secret key K and a secret key K_i to the PGDs in the groups G_i, $i = 1,...n$, which in turn means there can be no "computing a verification key V_i^{Dest} as a function of the secret key K_i" and using the verification key to create a digital signature for the indicia.

B. Incorrect Motivation to Combine

In addition to the fact that a combination of Baker and Cordery fail to teach or suggest all the limitations of claim 28, it is respectfully submitted that the Examiner also fails to state a prima facie case of obviousness because the motivation to combine the references stated by the Examiner is incorrect.

Repeating from the previous Office Action, the Examiner stated "it would have been obvious to of ordinary skill in the art at the time the invention was made to modify the method of Baker et al. to use the generated verification key to create digital signature for the indicia, and digitally signing[sic] the indicia by including the digital signature and other generated token[sic] on the indicia because it would allow other party[sic] to determine whether both keys can be trusted that they actually originate from the meter." Final Office Action page 6.

The present invention, however, provides an improved method for evidencing and verifying postage indicia in which postage validation is performed at destination distribution centers, rather than at originating distribution centers, and the verification keys, which are encrypted as a function of the destination, are only distributed to the

corresponding distribution centers. Thus, even if a destination center were broken into, the perpetrator would only be able to forge postal indicia for mail pieces destined for the particular destination. In addition, the key ID is also encrypted so that even if a perpetrator were to crack a verification key, the perpetrator would still have a problem identifying which verification key was obtained. In order to forge the indicia, the perpetrator must possess two keys, rather than one, a secret key that the PGD used to compute the key ID, and the verification key itself.

The Examiner's stated motivation to determine whether both keys can be trusted that they actually originate from the meter has nothing to do with increasing security of the evidencing and verifying postage indicia in the manner claimed.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
Strategic Patent Group

June 7, 2006

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38329
(650) 969-7474